Incentives and Information Security

R. Anderson, T. Moore, S. Nagaraja and A. Ozment

November 24, 2009

Motivation

- Many systems fail not ultimately for technical reasons but because incentives are wrong.
- When crucial information is missing or withheld from one of the principal players.
- Measuring information security poses additional challenges.
- The principals want to both optimize the security level as well as the investment associated in securing a software and the entire system.
    1. Misaligned Incentives
    2. Informational Asymmetries

Economics of Information Security : Misaligned Incentives

- Bank Frauds : U.S banks are liable for costs of card fraud. U.K, banks could often get away with lot less.
  Yet, UK banks spent more on security and suffered more fraud.
- Privacy failures in health care: Hospital directors and insurance agencies' interests not aligned with those of the patients.

Economics of Information Security : Informational Asymmetries

Games where one player has more information of the game state than the opponent or games where one player can make moves that become known only with a certain probability.

Types of informational asymmetries relevant to information security :

1. Hidden Action Attacks : Difficulty of observing other's activities facilitates some attacks.
2. Hidden Information Attacks : Caused by our inability to effectively measure the security of software.

Hidden-Action Attacks

Examples :

- Insurance - Reckless behavior on the part of the insured.
- Computer networks are naturally susceptible to hidden-action attacks : Routers drop packets or falsify responses to routing requests, redirect traffic to eavesdrop etc.
- Peer-to-peer networks : node can join, transact with any other and leave rapidly making observation and penalty unlikely.

Arises :
If the net gain in utility from deviation is greater than the expected penalty enforced when observation is unlikely and less than the expected penalty when observation is likely.

Possible Solution

- Changing the network topology : Use of clusters. Newly joining nodes establish confidence among cluster nodes before gaining access to outside nodes through existing group channels.
- Possibly inefficient, but using social networking to forge links between trusted friends or acquaintances instead of random assignment.

Hidden Information-Attacks

- Cause : Design and implementations flaws in commercial softwares
- Economics of the software industry provides little incentives to prevent this.
- Akerlof's study on the used car market is well suited for studying "market with asymmetric information".

Hidden Information-Attacks

- Cause : Design and implementations flaws in commercial softwares
- Economics of the software industry provides little incentives to prevent this.
- Akerlof's study on the used car market is well suited for studying "market with asymmetric information".
  - 50 good used cars worth $ 2000 each.
  - 50 bad cars worth $ 1000 each.
  - The sellers know the difference but buyers do not.
  - What is the market clearing price?

Hidden Information-Attacks

- Cause : Design and implementations flaws in commercial softwares
- Economics of the software industry provides little incentives to prevent this.
- Akerlof's study on the used car market is well suited for studying "market with asymmetric information".
  - 50 good used cars worth $ 2000 each.
  - 50 bad cars worth $ 1000 each.
  - The sellers know the difference but buyers do not.
  - What is the market clearing price?
  - Price falls to $1000.

Vendor's lack of incentive : Factors

- Buyers do not want to pay price for quality they can not measure, so only low quality vehicles get sold
- Similar to the software market.
- In some cases, even the vendors have insufficient and less than accurate information.

Vendor's lack of incentive : Factors

- Buyers do not want to pay price for quality they can not measure, so only low quality vehicles get sold
- Similar to the software market.
- In some cases, even the vendors have insufficient and less than accurate information.
- Consequence : Buyers do not want to pay extra and vendors do not want to invest more for secured products.

Akerloff's study : Quality vs Uncertainty

1. A new car may be good or a bad just as an used car.
2. The estimate of a car being a "lemon" changes after a period of use.
3. This causes an asymmetry in knowledge.
4. **Bad cars sell at the same price as good cars** : buyers do not want to pay money for a quality they can not judge.
5. But a used car cannot have the same valuation as a new car.
6. An owner of a good car can only not receive the true value of his car, but can not even obtain the expected value of a new car.

Akerloff's study : Quality vs Uncertainty

1. A new car may be good or a bad just as an used car.
2. The estimate of a car being a "lemon" changes after a period of use.
3. This causes an asymmetry in knowledge.
4. **Bad cars sell at the same price as good cars** : buyers do not want to pay money for a quality they can not judge.
5. But a used car cannot have the same valuation as a new car.
6. An owner of a good car can only not receive the true value of his car, but can not even obtain the expected value of a new car.

Conclusion : Bad cars can drive out new cars.

$$\text{Bad} \succ \text{Not-so-bad} \succ \text{Med} \succ \text{Not-so-good} \succ \text{Good}$$

No market exists at all!

Setting : Quality vs Uncertainty

Demand for **used** cars depends most strongly on 2 variables :

- Price p, Average quality μ
- Supply $S = S(p),\ \mu = \mu(p)$.
- At Equilibrium : $S(p) = D(p, \mu(p))$
- As price falls, quality falls : $p \propto \mu$

2 groups of traders :

$$U_1 = M + \sum_{i=1}^{n} x_i,\ U_2 = M + \sum_{i=1}^{n} 3/2 x_i$$

M is the consumption of goods other than automobiles. x_i is the quality of the ith car, n is the number of cars.

.

- Both types of traders are von Neumann-Morgenstern maximizers of expected utility.
- Group one has N cars with uniformly distributed quality x, $0 \leq x \leq 2$, and group 2 has no car.
- The price of "other goods" M is unity.

Income of type 1 trader (including car sales) is Y_1 and Y_2 is income of all type 2 trader.

$$U_1 = M + \sum_{i=1}^{n} x_i, \quad U_2 = M + \sum_{i=1}^{n} \frac{3x_i}{2}$$

$$D_1 = \begin{cases} Y_1/p, & \mu > p \\ 0, & \mu < p \end{cases} \qquad D_2 = \begin{cases} Y_2/p, & 3\mu/2 > p \\ 0, & 3\mu/2 < p \end{cases}$$

If $\mu = p/2$ $\qquad S_2 = 0$

then $S_1 = pN/2, \quad p \leq 2$

Thus total demand $D(\mu, p) = D_1 + D_2$ is :

$$D(p, \mu) = \begin{cases} Y_2/p + Y_1/p, & p < \mu \\ Y_2/p, & \mu < p < 3/2\mu \\ 0, & p > 3\mu/2 \end{cases}$$

Conclusion :

- But, with price p and average quality $\mu = p/2$, trade can not take place at any price.
- Even though **at any given price** between 0 and 3, there are type 1 traders willing to sell cars at prices at which type 2 traders are willing to buy.

Measuring Software Security

- Statistical
- Market Based Approaches
- Insurance Based Approaches

Market Based Approaches

- Buyers and sellers establish the actual cost of finding a vulnerability in software or estimate the security of software according to their own knowledge.
- Several organizations purchase vulnerabilities : provide the vulnerability information simultaneously to their customers and to the vendor of the affected product.
  Not socially optimum : they always have an incentive to leak vulnerability information without proper safeguards.

Insurance Based Approaches

Advantage :

- Premiums are assigned based upon a firms IT infrastructure and the processes by which it is managed.
- Over the long run, results in a pool of data.

Insurance Based Approaches

Advantage :

- Premiums are assigned based upon a firms IT infrastructure and the processes by which it is managed.
- Over the long run, results in a pool of data.

Disadvantage :

- Firms are physically and logically interdependent because cyber attacks often exploit a vulnerability in a system used by many firms.
- This makes certain cyber-risks unattractive to insurers especially where risks are globally correlated like virus or worm attacks.

Conclusion : Firms under invest in both security technology and in cyber insurance. Insurance companies must charge a higher premium because the risks are highly correlated. Thereby preventing vast majority of firms from adequately insuring themselves.